

**HEALTH CARE FINANCING ADMINISTRATION  
 FIVE YEAR INFORMATION  
 RESOURCES MANAGEMENT PLAN  
 (FY 2001 - FY 2005)**

***FOIA VERSION***

<b>I.</b>	<b>EXECUTIVE SUMMARY</b>	Page 1
<b>II.</b>	<b>STRATEGIC PLAN</b>	Page 3
	A. Strategic Planning Assumptions	Page 5
	1. Customer Service	Page 5
	2. Quality of Care	Page 5
	3. Program Administration	Page 5
	B. HCFA Mission and Organization	Page 6
	C. Program Goals and Information Needs	Page 7
	D. IRM Vision, Goals, and Strategies	Page 9
	1. Information Technology Strategic Vision	Page 9
	2. Business Needs	Page 12
	a. Customer Service Needs	Page 12
	b. Quality of Care Needs	Page 12
	c. Program Management Needs	Page 13
	3. Business Origins of HCFA's Legacy Architecture	Page 15
	4. Current Capabilities, Future Needs, and the "Gap"	Page 17
	a. Flexibility and Adaptability	Page 17
	b. Performance	Page 18
	c. Security	Page 20
	d. Maintenance	Page 21
	5. Strategy for Closing the Gap	Page 22
	6. Key Elements of the Vision	Page 23
	7. Summary	Page 24
	E. Major Strategic Issues	Page 25
	1. Realization of Conceptual Model	Page 25
	a. Development/Refinement of Core, Enterprise Databases	page 25
	b. Business Application Development/Reengineering	Page 26
	c. Migration toward Target Architecture Standards	Page 27

d.	Promoting More Effective Management of IT Investments .....	Page 27
2.	Security Posture Improvement .....	Page 27
3.	Systems Quality .....	Page 28
a.	Capability Maturity Model for Software .....	Page 28
b.	Quality Assurance .....	Page 31
4.	IT Training .....	Page 33
a.	Enterprise-wide IT Governance .....	Page 33
b.	Infrastructure Operations .....	Page 33
c.	Database Development and Management .....	Page 34
d.	Data Quality, Integrity and Standards .....	Page 34
e.	Security .....	Page 35
<b>III.</b>	<b>CAPITAL PLANNING AND INVESTMENT .....</b>	<b>Page 36</b>
A.	Investment Review Process .....	Page 36
1.	IT Review Boards .....	Page 37
2.	IT Review Process .....	Page 37
a.	Selection .....	Page 37
b.	Control .....	Page 38
c.	Evaluation .....	Page 40
3.	IT Database .....	Page 41
4.	Acquisition Management .....	Page 41
B.	Investment Portfolio .....	Page 41
1.	Current IT Portfolios .....	Page 41
2.	Presidential Decision Directive 63 .....	Page 42
3.	Best Practices .....	Page 43
4.	Other Major Highlights .....	Page 43
a.	Conversion of M204 Databases to Relational Databases .....	Page 43
b.	Quality Improvement & Evaluation System (QIES) .....	Page 43
c.	Medicare Managed Care Systems Redesign (MMCS) .....	Page 44
d.	National 800 Number Telephone Service .....	Page 44
e.	Medicare Contractor Integrated General Ledger Accounting System (IGLAS) .....	Page 44
C.	Capital Plans .....	Page 45
1.	OIS 300 - HCFA Internal Systems Security Initiative .....	Page 46
2.	OIS 414 - Medicare Contractor Systems Security Initiative .....	Page 47
3.	OIS 67 - Transition Legacy Systems .....	Page 48
4.	OIS 284 - Medicaid Statistical Information System (MSIS) Database Conversion to DB2 .....	Page 50
5.	OIS 467 - Beneficiary Database Prototype (BDP) .....	Page 51
6.	CHPP 403 - Collection of Managed Care Encounter Data and	

	Implementation of Risk Adjusters for Medicare .....	Page 52
7.	OIS - 285 National Medicare Utilization Database (NMUD) Conversion .....	Page 54
8.	OIS 139 - National Provider System (NPS) .....	Page 55
9.	CMSO 37 - Quality Improvement and Evaluation System (QIES) .....	
Page 56		
10.	CBS 106 - PlanID .....	Page 58
11.	CBS 143 - Telephone Customer Service Strategy .....	Page 59
12.	OIS 407 - Medicare Managed Care Systems Redesign .....	Page 60
D.	Information Technology Architecture (ITA) .....	Page 68
1.	Overview of the ITA Model .....	Page 69
2.	ITA Components .....	Page 69
a.	IT Direction .....	Page 70
b.	Business Architecture .....	Page 70
c.	Information Architecture .....	Page 70
d.	Application Architecture .....	Page 71
e.	Infrastructure Architecture .....	Page 71
f.	Security Architecture .....	Page 72
g.	Management and Governance .....	Page 72
3.	Future Paths .....	Page 73
4.	National Health Care EDI Standards and Identifiers .....	Page 74
E.	Automated Information Systems (AIS) Security .....	Page 75
1.	Policies and Procedures .....	Page 75
2.	Training and Administration .....	Page 76
3.	Systems Engineering .....	Page 76
4.	Oversight and Management .....	
Page 76		
F.	Performance Measurement and Evaluation Plan (PMEP) .....	Page 77
1.	Earned Value Management .....	Page 78
2.	Performance Based Contracting .....	Page 79
3.	Performance Measurement System .....	
Page 79		
4.	Earned Value Management Project Proposal Clause Statement .....	Page 80

## I. EXECUTIVE SUMMARY

Having successfully survived the larger part of millennium Y2K transition, the Health Care Financing Administration's (HCFA) information technology (IT) focus now shifts to addressing a twofold challenge: preparing HCFA to successfully implement HCFA's "information-centric" IT Architecture Model, and supporting the ever-increasing demand for IT solutions to carry out HCFA's strategic and business objectives.

HCFA has made substantial progress in developing its IT vision for the future and the architecture to support this vision. While the Y2K transition was a major and complex challenge for the Agency, it highlighted the central role IT plays in supporting our business operations. The Y2K experience, among other things, reinforced the importance of integrating IT capital planning and investment activities with our Agency strategic business objectives to ensure that limited IT resources are aligned with business priorities. Achieving Y2K compliance forced HCFA to delve into parts of our business at a level of detail not previously done. This expanded knowledge has provided an essential base for the IT architecture.

This Five Year Plan reflects HCFA's commitment to be a mature IT organization, based on the lessons learned from the Y2K experience and prior systems development initiatives. These lessons have shown us the need for a strategic IT vision and an IT architecture that support this vision and the value of having a strong IT investment planning and management process. We need to make sound IT investment decisions based on delivered value and return-on-investment and effectively manage IT investments using integrated project planning, requirements management, change control, independent testing and validation of solutions. We need an enterprise-wide systems security program to address the vulnerabilities and risks of our data and systems.

We discuss both our accomplishments to date in implementing these lessons learned (selecting investments through our capital planning and investment review process; planning and managing these investments more effectively), as well as our plans for future improvements (integrating planning activities and performance metrics, requirements analysis and change management, independent testing and validation and security requirements).

This Plan also reflects the critical role IT plays in supporting HCFA's accomplishment of business objectives and responding to legislative mandates. A central theme of HCFA's Strategic Plan is moving the Agency toward becoming a "beneficiary-centered purchaser" of health care services. Fulfilling this role requires that HCFA successfully integrate not only its more traditional role of regulator with that of payor, but it also requires us to place greater emphasis on assuring that expenditures on behalf of beneficiaries are warranted, prudent, and supportive of the providing quality care for beneficiaries at a reasonable cost. Implementation of the Balanced Budget Act (BBA) of 1997 (particularly the Medicare+Choice program and the National Medicare Education Program) and the Health Insurance Portability and Accountability Act of

1996 place new oversight and administration demands on us, primarily making information more readily available to beneficiaries for informed health care choices. Reducing fraud, abuse, and waste; improving oversight of Medicare contractors; strengthening oversight of health facility quality and safety - each of these major initiatives relies extensively on IT solutions. Integrating data and making it useful supports multiple levels of decision-making, HCFA's management of its programs, beneficiary health care choices, and research, to name a few.

The "information-centric" IT Architecture Model, outlined in the Strategic Plan chapter of this Plan, is the conceptual framework for managing our development of essential, core databases and their interfaces with business applications that will support these and other major initiatives. It remains the central vision for HCFA's IT program and IT architecture. We discuss this model and a number of the major projects and initiatives that help us move in the direction outlined in the model.

We also recognize the need for increased emphasis on ensuring that our data and systems are secure from unwarranted access and disclosure. HCFA's databases and systems are information-rich. As we re-engineer our central databases, our challenge is to ensure compliance with Presidential Decision Directive 63; that data is made accessible to only authorized users and that systems, networks, processes, data, and websites are secure from tampering, disruption, or unauthorized access or use. We discuss our plans for strengthening our systems security program (security planning, oversight, and assessment).

This Plan remains a living document, designed to outline our general direction for the next five years, but flexible enough to permit mid-course corrections as events and circumstances warrant. We hope this Plan provides our partners and stakeholders with a clear sense of where we expect our energies to be focused in the future, and challenges them to help us in accomplishing these strategic business and IT objectives.

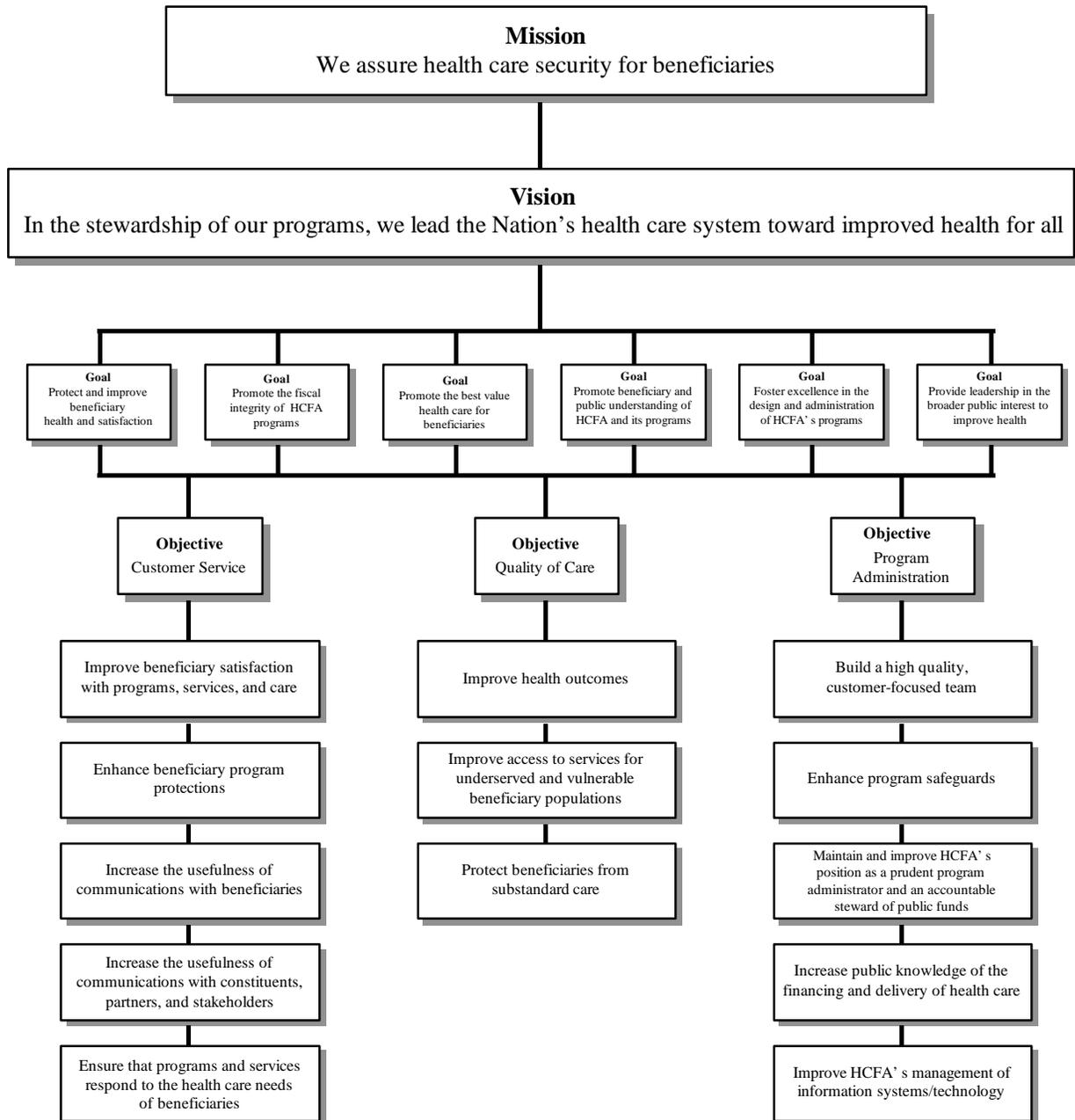
## II. STRATEGIC PLAN

HCFA's formal strategic planning process began several years prior to the publication of the Agency's first formal Strategic Plan in 1994. However, with increasing workloads and declining resources, we realized that our mission and future work needed to be further refined. As a result, HCFA embarked on a comprehensive self-study and consultation process in 1996 that resulted in a restructuring of the Agency in mid-1997. The restructuring entailed a reorganization of the Agency around its major "audiences" and a new, sharper statement of the Agency core work and future roles.

This process also formed the basis for the review of the Agency's Strategic Plan. The plan was revised in 1998 and the central theme is to move HCFA forward in becoming a "beneficiary-centered purchaser" of health care. The Agency is committed to expanding its role from a regulator and payor of claims to also be a prudent purchaser of health care services. HCFA will strive to use its market presence to obtain high value (quality at a reasonable cost) health care on behalf of Medicare and Medicaid beneficiaries. Another important theme is a heightened awareness of change in the larger health care environment in which HCFA operates and the need for flexible responses to those changes, especially those related to persons with disabilities and low-income populations.

The current Strategic Plan consists of six strategic goals and 13 objectives. Achievement of our strategic goals and objectives is assessed through our performance goals. Some goals will take several years to achieve and others will be a single year effort. Specific details about HCFA's performance goals can be found in the *HCFA FY 2001 Annual Performance Plan*. The Strategic Plan goals and the objectives that support those goals are illustrated in the chart on the following page. HCFA's IT planning processes are designed to identify IT investments that support the strategic goals and three major business drivers described in this plan: Customer Service, Quality of Care, and Program Administration.

# HCFA's Strategic Plan Goals & Objectives



## **A. STRATEGIC PLANNING ASSUMPTIONS**

### **1. Customer Service**

One of HCFA's assumptions about the future health care environment is that consumers will take a greater role in making decisions affecting their health care. This is especially true with the enactment of the BBA, under which beneficiaries have increasing options for tailoring their own health care system. HCFA will be exploring ways to better reach out to beneficiaries to ensure they understand their health care options and can make informed choices. Beneficiary satisfaction with the health care they receive is a driving force for change in the health care market. It is important that beneficiaries are aware of their treatment options, appeal rights, health plan choices, and health care benefits coverage. HCFA must also be positioned to better service our customers, both beneficiaries and providers, by providing access to timely and accurate information about beneficiary enrollment status, coverage of services, and payment for services. Implementation of HCFA's "information-centric" IT architecture model, outlined below, will allow HCFA to better support these goals.

### **2. Quality of Care**

HCFA is reinventing the way it monitors Medicare and Medicaid quality in both fee-for-service and managed care arenas. HCFA's role as an overseer of the care offered to its beneficiaries and as a leader for national quality standards and research demands world class quality of care information. A coordinated series of projects to establish national clinical information databases is underway to support the development of quality indicators and the oversight of the quality of care delivered to our beneficiaries.

### **3. Program Administration**

HCFA must be increasingly vigilant in its efforts to preserve the fiscal integrity of the Medicare program and to safeguard the Medicare Trust Fund. Accurate and consistent national data will allow us to monitor program expenditures and services rendered to prevent and to detect fraud and abuse. Through the use of the latest technology, such as electronic fraud detection software, Medicare bills and billing data are coming under much greater scrutiny; and systems planned for future use will increasingly include prepayment anti-fraud features. National databases will enable HCFA to apply new technology, including the new fraud and abuse algorithms and adapted COTS software. Over the longer term, the Medicare and Medicaid programs will expand application of these techniques. The Medicare Integrity Program IT investments will continue to enhance HCFA's program safeguard activities by allowing us to focus our resources more efficiently and effectively, improving our

data/information dissemination capabilities, and increasing our ability to identify potential program vulnerabilities at an early stage.

Our challenge is to create an information-centric IT environment that supports these business drivers by meeting the information needs of HCFA's customers and partners using subject-matter databases, user-friendly access structures, and efficient transaction processing systems.

## **B. HCFA MISSION AND ORGANIZATION**

As mentioned earlier, as a result of the comprehensive self-study and consultation process in 1996, HCFA was restructured in mid-1997 to support service to its major customer groups. Three centers focus on each of HCFA's primary audiences or customer groups -- beneficiaries, health plans and providers, and States. The centers provide "one stop shopping" for individuals and organizations interacting with HCFA. Other units with specialized expertise such as clinical knowledge, communications, and legislation, support the centers. Four field executives (Consortium Administrators) bring a local perspective to compelling issues. This structure allows us to fulfill our mission of assuring health care security for beneficiaries.

The Office of Information Services (OIS) is the organizational home of HCFA's Chief Information Officer (CIO), who is responsible for managing HCFA's IT assets including enterprise databases and operational systems. HCFA's 1997 reorganization provided the impetus to not only establish an Agency CIO, but just as importantly to restructure HCFA's IT components to meet the challenges of HCFA's evolving business environment. HCFA looks to the CIO to serve as an enabler for bringing the power of IT solutions to HCFA's business process to permit these business processes to be done in new, innovative, more efficient, and more effective ways. This means that the CIO must be fully conversant with the organizational needs and business drivers of HCFA's components and utilize that understanding to develop effective and efficient solutions within a strategic context of an enterprise information technology architecture.

The focus for the CIO cannot, however, be strictly internal. Not only must the CIO have an extensive and current understanding of technological capabilities, but that knowledge needs to be anchored in the larger context of HCFA's relationships with the public and key industries which help shape the HCFA business environment. HCFA must operate within and adapt itself to the realities of life in the industries of health care, insurance, banking, telecommunications, and information technology.

To support the CIO's role of developing an IT vision and carrying it out, HCFA's components are organized to provide both structure and discipline to IT processes. This organization:

- < Enables an enterprise-wide view of IT, a crucial prerequisite to the creation of an integrated information technology architecture;
- < Brings mission-critical field payment systems, the source of most of HCFA's data, under CIO control;
- < Establishes an organizational home for enterprise databases;
- < Facilitates the process of strategic information management;
- < Institutionalizes the function of establishing Electronic Data Interchange (EDI) standards for HCFA and nationally as required by HIPAA;
- < Establishes an organizational home for essential systems quality and change management activities; and
- < Provides for planning and management of IT investments as Agency assets, as required by the Clinger-Cohen Act and within the context of HCFA's Strategic Plan.

These changes position OIS not only to provide better support to the HCFA business units, but to participate actively in the formulation of strategic business plans.

### **C. PROGRAM GOALS AND INFORMATION NEEDS**

A central theme of HCFA's Strategic Plan is moving the Agency toward becoming a "beneficiary-centered purchaser" of health care services. This movement expands HCFA's role beyond its traditional regulatory and claims payment focus into one which places greater emphasis on assuring that its expenditures on behalf of its beneficiaries are warranted, prudent, and supportive of the overarching goal of providing quality care for beneficiaries at reasonable and proper cost.

HCFA needs to aggressively respond and adapt to the restructuring of traditional health care delivery systems and the organizations that support and control them. Increased emphasis on profitability in these structures drives the need for improved measures of quality of care and increased attention to health care outcomes to ensure that reduction in service costs do not imperil the delivered quality of care or the overall health of the beneficiary population.

Most succinctly, HCFA's mission is to pay for health care services to its beneficiaries. It is mandated to do this in two major programs, Medicaid and Medicare. Medicare is itself composed of three major parts, which differ from each other largely in the way that they pay for the services delivered to the beneficiaries.

Medicaid is a program that is operated by the individual States. HCFA has an oversight role in ensuring that the States follow certain guidelines, but has by law little direct business involvement in the claims process. HCFA's role is to provide a conduit for Medicaid trust

fund dollars to flow to the States, which directly manage the processing and payment of claims. States are also required to submit claims data to HCFA.

The Medicare program is managed directly by HCFA and through its contractors. The three major components in Medicare are largely structured parallel to the way the health care industry is organized. Medicare Part A encompasses payment for services provided by hospitals and other such centralized organizations. Medicare Part B encompasses payment for services from traditional fee-for-service providers, which include individual physician practices and suppliers of various specialized services and medical equipment. The third program is Managed Care, which contracts with managed care organizations and makes capitated prepayments to them for care to be provided to their enrolled beneficiaries.

Largely, these four programs (Medicaid, Medicare Parts A and B, and Medicare Managed Care) arose through separate legislation, and historically developed as separate business functions. However, the programs all use fundamentally similar processes, namely, eligibility is validated, a health care (or health care related) service is provided to a beneficiary, the service is validated, payment is made for the service, and statistics are collected. The chief differences in the programs lay in how the payment is calculated and in the timing of the payments relative to the time the service is delivered. In Medicaid, HCFA distributes money to the States. In Medicare Part A, bulk payments are made to providers (largely hospitals) prospectively, based upon historical patterns of service, and an annual reconciliation adjusts for any over- or under-payment. In Medicare Part A, hospital payments are made after discharge based on prospectively determined amounts. In Medicare Part B, payments are made directly to individual provider entities following the delivery of service or products. In the Medicare Managed Care program (now Medicare+Choice), providers are pre-paid, and they are expected to provide appropriate care to their enrollees on an as-needed basis. In each case records supporting the delivered instance of care are collected and are used to justify the cost of the individual or collective service. These records are archived and the information used in the development of policy which determines what kinds and amounts of service are allowed.

HCFA is not directly involved with health care delivery, but is wholly concerned with the policies that govern what services or products are covered, the management of the delivery, and ultimately the payment for the delivered products and services. Thus HCFA is centrally concerned with the management of flow of information (e.g., claims data, service statistics, service charges), and, using that information, with the development of policy to determine what services are covered. Thus, HCFA is a very information dependent organization; its primary business role is the collection, distribution, and analysis of information, and policy decision-making based upon the data analyses.

Our focus in this document is in how the business role of information management can best be performed by HCFA, remembering always that the ultimate goal of HCFA's programs is the efficient delivery of effective health care services to our beneficiaries. Before examining

the three main business drivers in detail, we will briefly enumerate some high-level characteristics.

Program Management:

HCFA's business operations need to perform at or better than current industry standard. In particular, the following are critical areas where information technology plays a role:

- < Efficiency - Business operations, such as claims processing, claims payment, contract management, encounter data collection, data analysis, and audit functions, all need to focus on optimizing value for expenditures.
- < Effectiveness - Program effectiveness is a measure of outcomes. The goal of HCFA programs is effective health care for its beneficiaries.
- < Security - Program operations must ensure that privacy information entrusted to HCFA is properly protected and managed against loss or corruption, and that processes and corporate assets are protected against damage or unauthorized use.
- < Continuity of Service - Business service needs to be protected from interruption. This implies mediation of risk through careful planning and prudent program and project management.

Customer Service:

HCFA's customers need timely access to accurate information about their benefits and eligibility, and they need accurate, timely, and complete responses to requests for service and information.

Quality of Care:

HCFA must maintain and, if possible, improve the quality of beneficiary medical care while ensuring that costs remain reasonable.

## **D. IRM VISION, GOALS, AND STRATEGIES**

### **1. Information Technology Strategic Vision**

Organizations employ IT to enable the management and flow of information in support of business needs. IT provides the tools for storage, access, movement, manipulation, and display of information, so that appropriate decisions can be made promptly and accurately. Some, but not all, decision-making can be automated, so one focus of the IT effort is to automate those rote and routine processes, reserving human effort for the most complex and demanding tasks. Simply, the goal of information technology is to leverage human activity.

Congress recognized the importance of taking a strategic approach to Government IT in the Clinger-Cohen Act. The Office of Management and Budget (OMB) has supplemented the statute with focussed guidance on a variety of IT-related topics. HCFA has responded to this environmental sea change by establishing a CIO position during its 1997 reorganization and implementing IT investment review procedures which internalize the so-called Raines' rules. Further HCFA established a Systems Architect position reporting to the CIO and awarded a series of blanket purchase agreement contracts for professional systems integration services. These steps position HCFA to deal effectively with the challenges it faces in acquiring and deploying IT to support HCFA's complex and evolving mission.

To promote the health of our beneficiaries, we wish to minimize administrative barriers to the delivery of health care while maintaining adequate oversight and control to ensure that the dollars are well spent. This means that queries to stored information, namely, the determinations of eligibility of beneficiaries and of providers, determinations of the validity of claims, and decisions on payments need to be performed very rapidly to avoid delaying actual delivery of care. If health care providers do not promptly receive payment, for example, we induce providers to remove themselves from the program, potentially denying beneficiaries needed care.

The highest volume business process that HCFA carries out involves the processing and payment of claims filed on behalf of beneficiaries by providers. A major IT challenge is to process and pay claims both rapidly and, more importantly, make the correct payment determination up front when the data volumes are immense. As there is substantial structure to the claim process, this function is identified in IT terms as an On-Line Transaction Processing (OLTP) function, which is fundamentally similar to, but far more complex than, processing credit card transactions.

Another significant function of HCFA relates to maintaining and providing health care information for decision-making. The advent of managed care and the structural changes in the health care industry away from traditional fee-for-service introduce new IT challenges, such as the collection of encounter data, assessment of quality of care outcomes, and direct information distribution to beneficiaries. As a Federal Agency, HCFA also has several other kinds of information customers, who have a need for and a right to information on HCFA's processes and procedures, and to access its data. These customers include oversight bodies such as Congress, the Office of Management and Budget, the General Accounting Office and the Office of the Inspector General; internal data customers and policy-makers in HCFA components; and external data customers including researchers and FOIA requesters. Although these information needs do not have the same time sensitivity or volume demands as claims processing, the information requests are more complex and less structured. This means that these data queries are more general, less easily automated, and require more resources per request. In IT terms, such query functions

are termed On-Line Analytical Processing or OLAP.

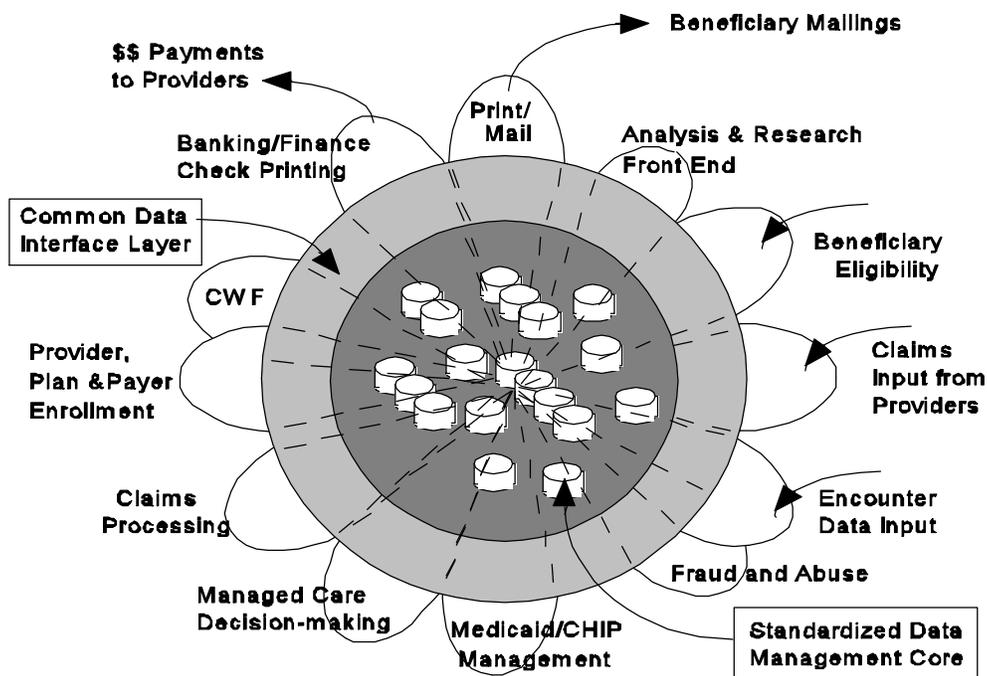
Our IT vision must accommodate and address the needs of both these important functions. The IT architecture, namely the combination of software systems, hardware platforms, and communications linkages, must not only handle current business needs, but must also provide the inherent capability to smoothly expand to address future volume needs, to seamlessly adopt new and more efficient technologies as they develop, and to readily support the administration of new programs.

Our IT vision thus starts with data management as the core process. All operational business functions can be seen as data operations, whether the function is claims processing, financial audits, or research queries. By optimizing information management we improve the efficiency of all processes dependent on information flow. This optimization depends upon structuring the data so that searches through the data are rapid, and upon structuring the interfaces to the data so that communication of data to and from business functions is efficient and well defined. This information-centric vision, visualized by a “sunflower” model, shown in Figure 1, encompasses the IT needs of all of HCFA's programs.

**Figure 1. Information-Centric Vision of Future HCFA Information Architecture.** Individual business functions are supported by specialized systems represented by the petals. Primary database management occurs in the core; all databases are readily accessible to all business functions through standard interfaces. The use of standard interfaces allows functions to be easily altered, added, or removed without affecting other operations. Compare this model to the Business System-Oriented Architecture of Figure 2. Note that this picture is a logical functional model and does not presuppose physical co-location of functional elements. The specialized business systems shown in this picture are a subset of the many programmatic and administrative systems extant at HCFA. Many more petals would be needed to make this a comprehensive model of the enterprise.

## 2. Business Needs

The “information-centric” vision addresses HCFA's current and future needs as follows:



**“Sunflower” Model for the Information-Centric IT Architecture**

### a. Customer Service Needs

#### Accuracy of Responses to Information Requests:

Integrating data used by all business processes does the following:

- < Improved synchronization of data enhances the accuracy of data responses.

- < Where data queries are filled promptly, outdated information is significantly minimized.
- < Eliminating replication improves data consistency and accuracy.

Timeliness of Responses to Information Requests:

Integrating data used by all business processes does the following:

- < Responses are more timely when the data is all accessible in one logical location.

Using standardized interfaces does the following:

- < Standardized interfaces allow staff to build ad hoc queries from their desktops, instead of requesting programmers to develop specialized reports; response times drop dramatically.

Completeness of Responses to Information Requests:

Integrating data used by all business processes does the following:

- < Responses requiring data from multiple sources tend to be incomplete when the data is not all accessible simultaneously; an integrated data store provides completeness by definition.
- < Data collated from separate sources often contain inconsistencies that cannot be reconciled by the requester; such inconsistencies are eliminated by data integration, making responses more reliably complete.

**b. Quality of Care Needs**

Maintenance of Quality of Care Levels:

Integrating data used by all business processes does the following:

- < Historic data can be effectively mined for outcomes and quality assessments when the data is integrated and readily accessible to program managers and policy-makers. Such baseline outcomes information is critical in determining whether levels of care are maintained at current levels by new service providers (e.g., managed care).
- < Integrated data makes possible comparative studies of the value of outcome indicators, e.g., encounter data, relative to prior collected data, in time frames short enough to affect policy decisions and allow proactive program management to prevent degradation of beneficiary health.

Improvement of Beneficiary Health:

Integrating data used by all business processes does the following:

- < Integrated data makes possible new policies, based upon statistical

outcomes and epidemiological studies not previously practical, that can improve health outcomes.

- < More efficient operations yield programmatic savings that can be spent profitably on outreach and educational programs that can lead to better use of health care benefits by beneficiaries.

### **c. Program Management Needs**

#### Increased Efficiency:

Integrating data used by all business processes does the following:

- < Replicate database management structures are consolidated and require less staff support.
- < Elimination of replicate data reduces overall storage needs and costs.
- < Synchronization problems between different copies of the same data in different business functions disappear, eliminating costly exception handling due to data discrepancies.
- < Consolidation of similar data input/output functions from different business systems reduces system maintenance costs and provides greater system stability and reliability.
- < Economies of scale result from use of common platforms as database servers.
- < Reduction in size of business function systems results in decreased testing and maintenance costs as complexity decreases.

Using standardized interfaces does the following:

- < Subsystems that perform different business functions become smaller, more modular, and easier to maintain and modify, which translates into decreased life-cycle costs.
- < Addition of new business functions is simplified because the functions build upon existing services; new subsystems are smaller and thus faster and cheaper to build, test, and maintain.

#### Increased Effectiveness:

Integrating existing data used by all business processes does the following:

- < Pre-payment detection of fraud, waste, and abuse is facilitated.
- < Costly investigations are focussed due to more accurate targeting of suspicious claim behavior.
- < Data integration improves post-payment analysis of health care outcomes leading to enhanced policy development.
- < Financial data can be more readily analyzed to support program management, detect operational inefficiencies, and perform reliable cost-benefit analysis.
- < As data becomes more readily accessible, and more used, the quality

of the data is improved, leading in the long term to more accurate decisions and more effective programs.

Using standardized interfaces does the following:

- < Electronic data exchanges in support of claims adjudication permit, for example, resolution of suspended claims by automated requests for structured supplemental data directly from providers' information systems. This substantially leverages the efforts of medical reviewers.

Increased Security:

Integrating data used by all business processes does the following:

- < Risks of disclosure or corruption of privacy information can be more effectively addressed when data is under centralized control, and when there are fewer copies of the data to protect.
- < Security policies are easier and cheaper to enforce.
- < Risks to processes and resources are more readily addressed in an integrated environment.

Using standardized interfaces does the following:

- < More structured interfaces vastly simplify detection of illicit and illegal behavior.

Continuity of Service:

Integrating data used by all business processes does the following:

- < Contingency and disaster planning are vastly simplified.
- < Increased security lessens threats of disruption of processing by illicit activity.
- < Operational stability is enhanced and system reliability is increased whenever systems are made less complex.

Using standardized interfaces does the following:

- < Risks and problems in transitioning workloads between contractors decrease with increased standardization.

In summary, by creating centralized, standardized data stores, HCFA can ensure reliable and consistent results each time the data are accessed. This structure allows for increased understanding of the data by its users since there is a single source of the data elements as well as a comprehensive definition of the origin, meaning and uses of each data element. Additionally, a single store will allow for quick problem recognition, quick resolution of data errors, and for identification and explication of

data anomalies.

While for simplicity the discussion in the following sections is focussed primarily on the Medicare business processes and systems, similar cases can be made for HCFA's other program and administrative systems.

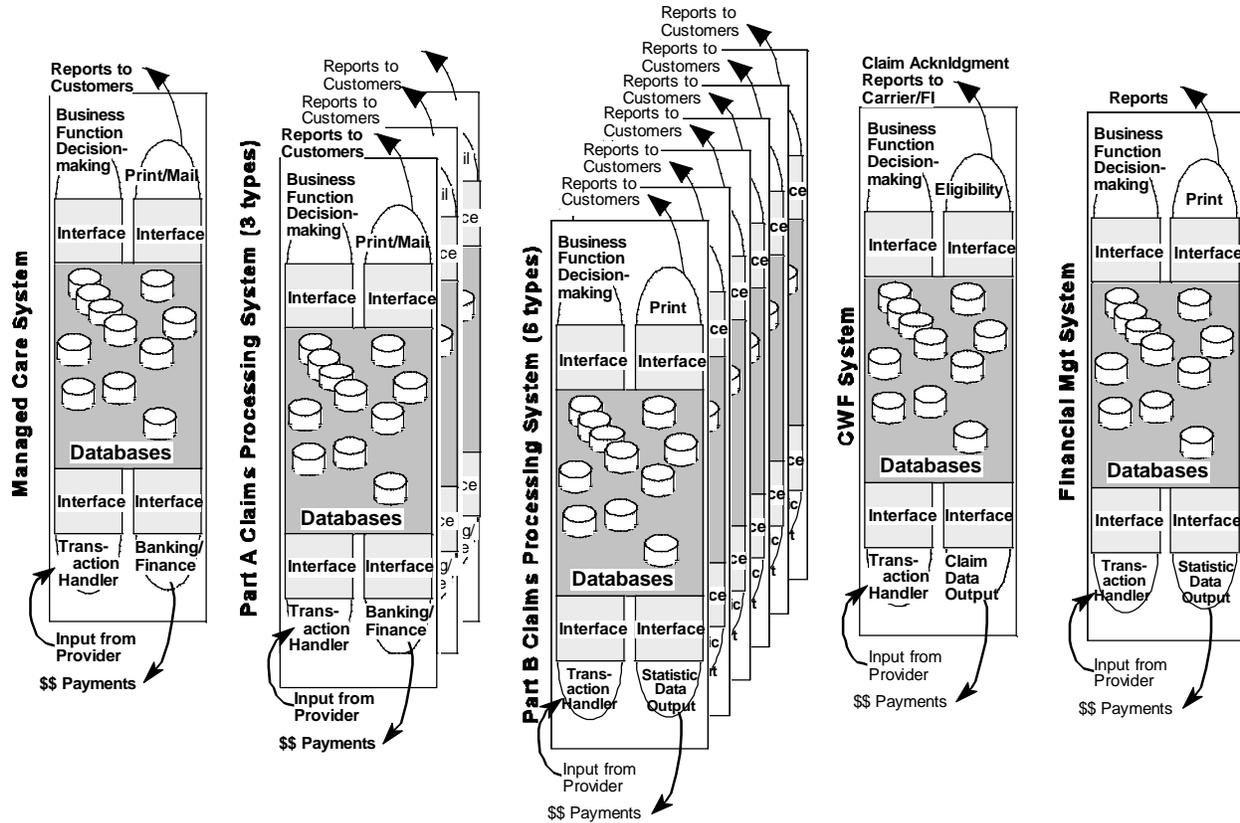
### **3. Business Origins of HCFA's Legacy Architecture**

HCFA's current IT architecture is a classic legacy operation, or worse, a collection of more than a hundred legacy operations, some of which are depicted by the "stovepipes" of Figure 2. By "legacy," we mean that the information systems, both software and hardware, still clearly reflect business and system design philosophies of an era when, for example, claims processing was largely a paper-handling function. At the time these systems were designed, automation was seen as a means of doing the same manual tasks, just more efficiently. To understand why HCFA's IT infrastructure has remained legacy, one must understand the historical forces that shaped it, and these are the forces which still impede modernization.

When the Medicare program was being defined, Congress saw it both as expedient and efficient to build the program around the capabilities of commercial medical insurance companies, which already possessed the skillsets for reviewing and paying medical service claims, at the time mainly a paper-based activity. Thus, Medicare's claims processing infrastructure was early institutionalized as a collection of many independent and local claims processing centers. It was simply cheaper to make use of the contractors' already-developed individual claims handling processes and mechanisms rather than invent and require the use of "Federal" processes.

As automation became more available, each claims processor was essentially free to develop its own IT implementation to support and execute HCFA policy. From the beginning HCFA itself focussed on policy analysis and contract management, leaving business operations, and thus most IT investment and planning, to the industry. The accepted model of the IT environment was of distributed and isolated systems that were not required to interact or intercommunicate, and that were allowed to develop independently of each other. Being derived from many different commercial systems and claims processing models, the only common IT design thread was one of enforcing a common policy.

**Figure 2. Business System-Oriented Architecture for Larger Medicare Programs.** In this architecture each business function is represented by a separate monolithic (stovepipe) system. Databases are not shared, although much of the data accessed is identical to data used by other business systems. While each system is stand-alone, there is much replication of functions. Yet, as each system is managed independently by different business units, common system functions will diverge



over time and the systems will be unable to communicate with each other despite their common origin. Nevertheless, systems are not truly separate because of interdependencies of replicated operational data.

Unlike government, the motivators for businesses to embrace new technology are simple: reduce costs by deploying cheaper or more efficient means of production, and gain new capabilities that permit new profit-making activities. Driven by the possibilities of increased profitability, business willingly accepts the risks of promptly investing in new technology and invests in detailed project planning and monitoring to control risk. In contrast, governments have been extraordinarily conservative (risk averse) in the short term, relying upon rote compliance with detailed contract terms to control risk, and remaining relatively insensitive to the business possibilities of new capabilities. Government agencies often have difficulty changing course because of broad impacts they have on the economy and because of the risk of adverse public reaction. Continuing on the current path, however ill-suited to the business needs, is often perceived as representing the least risk. Change is at best incremental and but a small deviation from the current path, as the status quo is most easily defensible.

Thus, current Medicare processing systems and HCFA central office IT infrastructure remain substantially similar to the technology implemented 10 to 15 years ago, despite operating on newer equipment.

Government legacy systems are large, monolithic, single-purpose software systems designed around “stovepipe” business functions. The software programs generally consist of millions of lines of aging COBOL code, (COBOL is a business programming language first developed in the fifties and sixties), were designed using decades-old hardware capabilities and software design concepts prevalent at the time, do not intercommunicate with other systems, run as batch (as opposed to interactive) processes, and are increasingly expensive and difficult to maintain because of the lack of adequate documentation and personnel skilled in the older language methods and programming styles. At HCFA Central Office, most of the systems are written in COBOL, but a significant fraction of the 17.6 million lines of systems code are written in the Model 204 database language, a language that is now largely abandoned in the United States.

#### **4. Current Capabilities, Future Needs, and the “Gap”**

There are significant gaps between HCFA's current and future business needs and the performance of its current IT infrastructure. We will now briefly describe five categories of gaps, namely in the areas of Flexibility and Adaptability, Performance, Security, Maintenance, and Service.

##### **a. Flexibility and Adaptability**

The current software infrastructure is increasingly difficult and expensive to maintain, much less expand to add new functionality to address new business needs. These systems were developed many years ago in languages in vogue at the time, to serve business needs strongly limited by the available technology. They have been incrementally modified over time, not to change the fundamental structure of the systems, but to add marginal capabilities and capacity. Further, the systems are inadequately documented. Even small changes are difficult, requiring substantial reexamination of the code and extensive testing to ensure that the changes do not propagate in unknown ways with unknown effects.

For life-cycle cost effectiveness the current HCFA software infrastructure needs to be more readily modifiable and adaptable. In its current legacy form, a major rebuild of a monolith may require five years or more. Because of short deadlines of mandated changes, as in those of the BBA, and the short cycles of technological evolution, a response time on the scale of one year is necessary. Otherwise the enterprise is denied the benefits and potential savings of using

improved technology and beneficiaries do not promptly receive the services of newly mandated programmatic changes.

**b. Performance**

The goal of deploying IT must be to leverage intellectual activity. Productivity gains permit more staff to be devoted to tasks that cannot be automated and that require more creative activity. HCFA's current business operations include many operations that rely excessively upon manual activity.

Program Integrity:

Program Integrity seeks to ensure that only claims that provide health care value to the beneficiary are paid, and paid at proper rates. Current Medicare systems focus on correctness of individual claims, deferring most review for medical necessity and fraud, waste, and abuse (FWA) detection for more human intensive, and thus very expensive, post-payment analysis. FWA that occurs at higher levels of aggregation, such as collusion, "ping-ponging," or bulk claim fabrication, is not readily detected by existing pre-payment processing mechanisms. The lack of significant pre-payment FWA detection forces HCFA to put undue reliance upon "pay-and-chase" methods. However, implementing the desired pre-payment FWA decision tools in the current environment requires that the data to support the decision tools be accessible interactively to those tools and that proven FWA detection algorithms be available.

The data to support such program integrity decision tools need to be global and timely. Currently, the National Claims History (NCH) database, HCFA's only global claims history database, does not contain all of the data needed for credible FWA detection, nor is the data it does contain readily accessible. More relevant information resides at contractor sites, in their local legacy environments; however, much of this information is lost when claim information is forwarded to the NCH. Most pertinently, claims were, until very recently, recorded as having been either paid or denied, but information as to whether the claim was determined to be FWA was not saved. Another failing is that "developed" or supporting information from review or investigations are not saved with the NCH claim record. Supporting record information, primarily in paper form, is kept only at the local contractor sites, and is accessible only for a short period before being archived in paper or microfilm.

By timely availability of information, we mean that all of the information relevant to the correctness of a claim be promptly available at its time of processing. In Medicare, a claim may be submitted as long as 27 months after the service was rendered. Closely related claims, as for a hospital stay and doctor visits to the patient while in the hospital, may be received months apart,

creating an environment ripe for abuse and fraud. Were this information available electronically and immediately upon the suspension of a questioned service claim, the claim might then be quickly adjudicated, perhaps in an automated or semi-automated way.

The data in the NCH is not readily accessible. A complex query against the NCH can require several months to process. This is because the database is a “flat file,” consisting of many “one-line” claim records (all the information pertinent to one claim exists in one “line” in the file, requiring a linear read of every full record in the file to extract just the information of interest).

Although we have focussed here on the NCH as HCFA’s main repository of historical Medicare claim data, the situation with other HCFA program data are similar; data stores are not readily accessible to queries, the data may be incomplete or contain inconsistencies, and may not be up-to-date, hampering decision-making. Further, cross-correlation of information across different legacy systems is time-consuming and difficult.

#### Policy and Decision Support

The goal of Policy and Decision Support is to provide timely answers to such questions as: What is the projectable cost of extending coverage to include acupuncture pain management for outpatient surgery? What health implications result from changing the allowed frequency of ESRD (End State Renal Disease) patient dialysis treatments to no more than once every four calendar days? Such questions are often asked during Medicare and Medicaid policy development, whether by HCFA policy staff, Congressional staff, State agencies, or university health care delivery researchers. As noted above, retrieval of raw data to generate statistics in order to answer such questions may take months. By the time the data is assembled, the interest and motivation that drove the question may have long ago faded. Worse still, delays in gathering the proper information result in delayed policy decisions that may negatively impact beneficiary health. Proper IT tools, such as those that model outcomes can reduce the time it takes to perform demonstrations.

#### Customer Service

Beneficiary requests for information or decision are handled both by Medicare contractors and at HCFA Central Office (CO) and Regional Offices (ROs). Queries range from what benefits are available to a particular beneficiary to requests from Congressional oversight committees for program statistical information. Response time to such inquiries is constrained by the difficult access to stored information. ROs rely upon interactive data query support of CO databases. Simple queries, such as of an individual beneficiary's eligibility status, may have sub-minute response times, while more complex queries; e.g.,

to support policy decisions requiring legislative action, may require up to several months. Because consumers are now accustomed to immediate response to their queries of the telephone company or airline reservation clerks, they reasonably expect similar responsiveness from government agencies.

A second “gap” is in the amount and type of data securely accessible by beneficiaries using convenient kiosk, web, and Internet tools, an area where HCFA lags far behind commercial entities.

Annually, HCFA CO receives more than thirty thousand data requests. These range from requests for a single summary statistic, such as the frequency of a particular psychiatric procedure in a given metropolitan area to a fraud investigation request for all Medicare claims for a given specialty across a dozen States. Given legacy structures of current HCFA databases and their access control software, such requests may require weeks of expensive programmer time and consume significant data processing resources to satisfy. This programming effort is often committed to satisfying a one-time request; the software will never be used again. If adequate security controls were in place to ensure the protection of privacy and were the data accessible by standard database query languages, the requests could be made directly by the requester, and responded to automatically by the HCFA database infrastructure, without the necessity of time-consuming, complex, one-time programming efforts.

We can summarize the above discussion into four database performance gaps:

- 1) critical claim data is currently not all in one place but is physically widely distributed, hindering and delaying access,
- 2) data already in HCFA databases is not, in general, organized to be readily available in a timely way,
- 3) data that is available is not the necessarily the correct data to support FWA, medical necessity, and policy making decisions, and
- 4) data is not readily or efficiently accessible from the databases that do exist.

### **c. Security**

The health care environment in which HCFA operates is changing rapidly and significantly. To meet the challenges in this new environment, HCFA has increased its reliance on networked systems which in turn have posed new security and other risks. HCFA has also increased the number of health care partners with which it works. At the same time, the complexity of the technology HCFA must use to function successfully in the new environment has increased. Given this rapidly-changing environment, HCFA leadership has increased its expectations for the level of acceptable security protection of

HCFA data. This has led to a number of assessments of the state of HCFA's systems security program over the past several years, both as a result of audits performed under the auspices of the Office of the Inspector General (as required under the Chief Financial Officers (CFO) Act of 1990) and from self-assessments by the Office of Information Services (OIS).

As a result of the various security assessments of HCFA's protection measures, a number of security vulnerabilities have been identified. Left uncorrected, they could result in:

- < The disclosure of beneficiary health information;
- < The disclosure of proprietary cost information of competing health plans and contract information;
- < Loss of integrity (correctness) of eligibility and payment information;
- < Denial of availability of IT resources to conduct the Agency's business; and
- < Loss of the Citizenry's trust in HCFA.

While it is difficult to completely eliminate all vulnerabilities or risks associated with unauthorized access or use of HCFA's data systems, the assessments highlight the importance for HCFA to further bolster its enterprise systems security program. As HCFA moves further into on-line activities, the protection of confidential information held in trust for the public becomes increasingly at risk. While there are no known instances where denial of services or compromise from disclosure of sensitive data has occurred, one instance of such an event would be unacceptable and could erode public confidence in HCFA's ability to properly fulfill its operational and stewardship responsibilities.

In identifying its security vulnerabilities, HCFA has learned that there are no quick fixes. Efforts have been made to remove the immediate known risks, to identify the root causes of the problems, and to conduct broad assessments to learn in depth HCFA's security shortcomings. HCFA has also taken steps to build an enterprise-wide capability for providing adequate long-term security safeguards that will allow HCFA to use technology to meet its business goals with confidence.

#### **d. Maintenance**

A significant HCFA expense is the maintenance of its current software. Largely, the system programs are written in older computer languages, are structured for a batch-processing environment, are poorly documented or undocumented, and have been so patched that the original program coding design is no longer recognizable. Such applications are seldom as efficient as originally designed.

When originally written, coding and data standards were probably nonexistent. For example, a HCFA software system, such as the 1.3 million line Managed Care system, can have hundreds of data references to dates. Because such a large system has dozens of smaller program modules, written at various times by different staff, many of the date references may be, for example, to the same “date-of-first-eligibility” of a managed care plan, which are stored under a variety of different variable names, and in different formats. This creates a maintenance nightmare, as any changes to the system require that the specialist programming the change be knowledgeable about the details of the whole system in order that all references to a particular datum are updated. Much time is lost researching whether a single planned change might have undesired consequences. Modern programming methods and the adoption of data naming and reference standards can significantly reduce the life-cycle costs of software. Were such standard practices already in place, the resolution of the millennium problem would be simple and orders of magnitude less expensive.

## **5. Strategy for Closing the Gap**

This IT Strategic Plan has two main thrusts: First, as Medicare and Medicaid today constitute some twenty per cent of the national expenditures for health care, it is vital that HCFA avoid any significant disruption in its processing and funding operations. Thus, a primary goal of the Agency must be on continuous, effective, and efficient operation. Recent legislation such as the BBA and Health Insurance Portability and Accountability Act (HIPAA) established new, time-sensitive expectations on HCFA, requiring it to add new services and products for its customers and to operate in more businesslike ways. Current operations must respond promptly to address urgent new and time-sensitive demands, even as HCFA works toward the target architecture.

Second, the very size and complexity of HCFA's IT enterprise demand a coherent long-range plan and vision if the enterprise is to evolve into a more efficient and capable operation. Computer, network, and communication technologies are evolving so rapidly that without careful long-range planning and implementation, the enterprise will not be able to take optimal advantage of new technologies, but rather will adopt technology haphazardly and in pieces that may not interoperate. This will likely expose the Agency to new security risks and threats. Given the size, distribution, and critical nature of HCFA's program management and payment operations, software and communications demands are very complex. Thus, development projects for such IT resources are complex, require external advanced technical efforts to develop, and will require significant, dedicated financial, personnel, and managerial resources for their success. Coherency of the products and the environment, consistency with business needs, both current and future, and successful implementation mandate long-range strategic IT planning and investment. The Clinger-Cohen Act reinforces this simple but fundamental business need to operate with rational IT investment

processes by giving directive and force of law as additional impetus. The strategic vision outlined in this document is HCFA's first step in performing this long-range IT planning process.

## **6. Key Elements of the Vision**

We have described above an Information Technology Vision that satisfies HCFA's business needs. Figure 1 is a picture that provides a high level, logical (as opposed to physical) architecture. The key elements of this picture are:

- 1) A central core of well-managed databases.
- 2) A structured interface that facilitates and modulates access to data in the core databases (this can be viewed as "middleware").
- 3) An assembly of modular application systems that manage infrastructure inputs and outputs, provide support for data operations (query, statistical analysis, data mining) and facilitate program operations.
- 4) A unified set of security services that safeguards the confidentiality, integrity, and availability of HCFA's assets.

As discussed in the gap analysis above, the legacy environment depicted in Figure 2 cannot satisfy many of HCFA's current business needs. Thus, perpetuating the status quo is not a viable option; the legacy IT environment is not sustainable.

There is a spectrum of options for replacement of the current environment. At one end of the spectrum of replacement strategies is wholesale system replacement, i.e., discarding the current IT environment and replacing it with a completely new one. This approach assumes that little of the current system has lasting value, that the ability and substantial resources are available to effect an en masse reconstruction and replacement, and that the risks involved both in the construction of the new system and the transition from the old to the new can be adequately managed. Introduction of cutting-edge technology also carries its own risk, which we term technical risk. A prime underlying assumption of this approach is that the quick availability of the entirely new functionality is worth the up front expense.

The other strategy extreme is a purely evolutionary and drawn-out piecemeal system replacement. This approach assumes that significant portions of the current structure have lasting value, that necessary resources will be available only over a long term, and that the cost of lost opportunity is not large. Because the pace of change is slower, the technical risk is small (by the time technology is fielded, it is no longer "new," but is well tested) and the capability requirements are lower. But if the infrastructure is already outdated, there is risk in being unable to quickly respond to changing business needs and to take prompt advantage of new and more efficient technologies. If the infrastructure is current and up-to-date, and is already modular

with well-defined interfaces, evolutionary changes produce the most manageable risk profile. Testing is easier on smaller, less complex modules than on large, and using standard interfaces limits unpredictable ramifications.

The key elements in deciding upon an optimal approach from this spectrum are cost of the replacement, cost of perpetuating current system or system components while the replacement is in progress, time-value of new capabilities, complexity cost, technical risk, and program management risk (including political risk). In general, monolithic replacement is justified where the existing system is structurally limiting, as legacy systems generally are, because the existing foundations fail, sometimes catastrophically, under increasing operational demands. A purely evolutionary replacement approach functions well if the system is already modular and possesses highly defined interfaces; aging modules can be replaced without causing unexpected disturbances or ripple effects elsewhere in the structure, and modules can be relatively easily rearranged to form a new structure, allowing adaptability, because of the standard interfaces. Given HCFA's current legacy environment on the one hand, and its pressing business need to readily implement new programs on the other, neither extreme is viable.

## **7. Summary**

Within the broad range of intermediate courses, we must pursue a course that balances return against resource cost and risk. The "sunflower" vision stresses central well-managed information management at the core with modular decision-making systems readily accessing any necessary data in the core. The vision design encompasses prompt as well as broad access to data, high reliability, and "maneuverability" to provide flexibility to quickly respond to future needs and to future technologies. A key element of the vision design is that multiple plausible paths for achieving the target architecture exist.

The vision and approach described in this document differ significantly from earlier HCFA IT investment efforts. The major difference is primarily one of approach and methodology. Instead of focussing upon a direct replacement of a major business function, the strategy we describe here is intended to address the business needs of the whole enterprise, and to chose IT investments that optimally move the IT infrastructure toward goals that support all of the enterprise business functions. The strategy follows an overall risk adverse approach, using incremental builds of highly structured code modules, standard interfaces, triage and object reuse where appropriate, and prudent project management processes. Frequent milestones and monitoring of project progress and deliverable quality with a variety of metrics are necessary to ensure successful development.

The sunflower vision represents a new IT goal for HCFA, that of an enterprise-wide

evolutionary IT environment. The philosophy naturally embraces the structured IT investment strategy of the Clinger-Cohen Act and of Raines' Rules.

## **E. MAJOR STRATEGIC ISSUES**

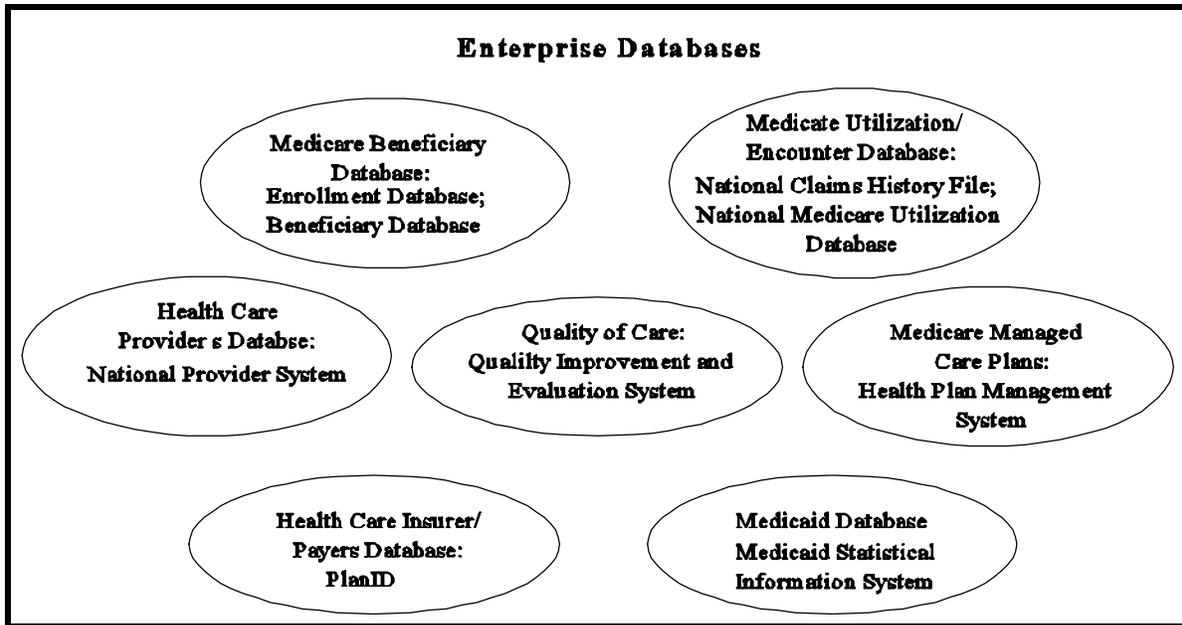
HCFA is faced with a number of strategic issues that affect its ability to carry out the Strategic Plan.

### **1. Realization of the Conceptual Model**

As HCFA moves forward in developing responses to key business objectives, IT solutions play a critical role in supporting these objectives. The “information-centric” IT architecture model, outlined earlier, is the conceptual framework for managing our development of essential, core databases and their interfaces with business applications to support major business objectives. There are several parallel strategies that we are deploying to realize this conceptual model, including the development/refinement of our core enterprise databases, business application development/reengineering, migration toward our target architecture standards, and promoting effective management of our IT investments.

#### **a. Development/Refinement of Core, Enterprise Databases**

Effectively supporting HCFA’s major business operations (within its Business Function Model) requires that we maintain easily accessible, valid, and reliable data and information for a number of events/entities. While there are multiple levels from which to view these data and information needs, at a high level, one can depict HCFA’s enterprise data model as follows:



Note: The databases identified for these major categories are not intended to be a complete inventory of the data repositories for each category. Similarly, a number of these databases are under various stages of development/prototyping.

Therefore, one of our strategies will be to continue development and refinement of these core, enterprise databases designed to support major business operations.

**b. Business Application Development/Reengineering**

Many business applications were designed ten or more years ago, when program requirements and/or transaction volumes were significantly different. Many were developed using programming or database structures that no longer provide ease of functionality and maintenance; nor the ability to easily adapt to changing business needs or legislative requirements. Similarly, as program requirements changed over time, many of these applications have become a patchwork of modules, fixes, etc. that make ongoing maintenance difficult (and costly). This makes modifications to handle new functions or programs difficult, expensive, and time-consuming

Therefore, we are undertaking a number of reengineering efforts to ensure that our business processes are effectively designed to meet current and future business needs; as well as ensuring that we have IT solutions effectively supporting these re-engineered business processes. Examples of these reengineering efforts include: redesign of the Medicare Managed Care Systems;

assessment and redesign of the Common Working File (CWF); and development and implementation of an integrated general ledger accounting system (IGLAS) for our Medicare fiscal contractor systems and redesign of the central HCFA financial accounting system. These projects are discussed later in this Plan.

**c. Migration toward Target Architecture Standards**

With the continuing development and specification of HCFA's IT architecture standards, we will be undertaking planned migration efforts toward these standards. For example, HCFA had made the decision several years ago to move toward a modern relational database structure (and away from, for example M204). The migration of databases will continue, in a phased approach, based on business and budget considerations.

**d. Promoting More Effective Management of IT Investments**

This is a multifaceted strategy designed to ensure that (1) IT investment decisions comply with the Clinger-Cohen Act, OMB guidance (including "Raines' Rules"), and sound investment decision-making principles; (2) systems development projects are developed consistent with industry standards (i.e., Software Development Capability Mature Model); (3) IT investment projects are managed effectively (using such disciplines as integrated project planning, earned value management reporting from contractors, and performance-based service contracting strategies).

**2. Security Posture Improvement**

Both health care and IT environment in which HCFA operates changes constantly. HCFA is relying more and more on networked systems, we have expanded our number of external partners, technology changes rapidly and is increasingly more complex, and there is a higher expectation of HCFA leadership in security at a national level. Our challenge going forward is to provide greater access and flexibility, while guarding against the intensity of existing threats and new threats because of increased connectivity and greater numbers of data users.

Our strategy is to achieve a sustainable and effective system and network security posture. We would not be able to administer our programs if system security flaws cause failures in continuity of program operations, protection of the privacy of beneficiary data, or protection of business-sensitive financial data. HCFA will take a two-pronged course of action: 1) continual assessment and correction of vulnerabilities, and 2) development and implementation of

user-transparent administrative, physical, and technical controls to adequately protect systems, networks, processes, and data.

This will be done with through the Systems Security Initiative, which will integrate security into our business and IT management processes. We will be both reactive in assessing and addressing known vulnerabilities and proactive by building security into new environments. Our systems security management program focused efforts in four areas: policy and procedures, training and awareness, security systems engineering, and management and oversight. These areas are discussed in detail in Section E of the Capital Plan, Automated Information Systems (AIS) Security.

### **3. Systems Quality**

#### **a. Capability Maturity Model (CMM) for Software**

The analysis, renovation, and testing conducted for Y2K uncovered many issues and practices that revealed a need for software development process improvement (SPI). The Agency recognizes the need to standardize the method of software development in order to improve results. We are planning on implementing the Software Engineering Institute's (SEI) Capability Maturity Model (CMM) for Software. Specifically, HCFA's new software process improvement goal is to achieve the Capability Maturity Model (CMM) for Software Level 2 Maturity Rating within the next three years. The CMM for Software is a framework that describes key elements of an effective software process. It covers practices for planning, engineering, and managing software development and maintenance. When this organizational model is followed, these practices improve the ability of organizations to meet their goals for cost, schedule, functionality, and product quality.

CMM describes a set of processes that result in more efficient and effective software development efforts and is intended to help software organizations improve the maturity of their software processes.

The CMM guides software organizations that want to gain control of their processes for developing and maintaining software and to evolve toward a culture of software engineering and management excellence. It is a description of the stages through which software organizations evolve as they define, implement, measure, control, and improve software processes.

The CMM model is composed of five maturity levels that define an ordinal scale for measuring the maturity of an organization's software process and for evaluating its software process capability. CMM for Software also help organizations prioritize its improvement efforts. This model provides a guide for

selecting process improvement strategies by facilitating the determination of current process capabilities and the identification of the issues most critical to software quality and process improvement. The CMM establishes a yardstick against which it is possible to judge, in a repeatable way, the maturity of an organization's software process and compare it to the state of the practice of the industry.

The maturity framework provided by CMM establishes a context in which:

- < Practices can be repeated. There are policies, procedures, and practices that commit the organization to implementing and performing consistently.
- < Best practices are defined sufficiently to allow for transfer across project boundaries, providing standardization for the organization.
- < Variations in performing best practices are reduced. Quantitative objectives are established for tasks; and measures are established, taken, and maintained to form a baseline from which an assessment is possible.
- < Practices are continuously improved to enhance capability (optimizing).

The CMM is built upon a framework of five increasing maturity levels. As organizations establish and improve the software processes by which they develop and maintain their software work products, they progress through the levels of maturity. Each maturity level provides a layer in the foundation for continuous process improvement. Achieving each level of the maturity model institutionalizes a different component in the software process, resulting in an overall increase in the process capability of the organization. Organizing the CMM into five levels prioritizes improvement actions for increasing software process maturity. The five maturity levels of CMM for Software are:

Level 1: Initial Level - (This is HCFA's current level). At the Initial level, the software processes are characterized as ad hoc, and occasionally chaotic. Few stable processes are defined and success depends on individual effort and heroics.

Level 2: Repeatable Level - Basic project management processes are established. Cost, schedule, and functionality are tracked and reported. The necessary process discipline is in place to repeat earlier successes on projects with similar applications.

Level 3: Defined Level - The software processes for both engineering and

management activities are documented, standardized, and integrated into a standard software process for the organization. All projects use an approved, tailored version of the organization's standard software process for developing and maintaining software.

Level 4: Managed Level - Detailed measures of the software process and product quality are collected. Both the software process and products are quantitatively understood and controlled.

Level 5: Optimizing Level - Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.

HCFA's immediate Software Process Improvement (SPI) goal is to achieve the Level 2 maturity rating. At Level 2 process capability is enhanced by establishing basic project management (tracking and reporting costs, schedule, and functionality) is established for each project. Processes are repeatable, so that planning and managing new projects is based on experience with previous projects. Projects implement effective processes that are defined, documented, practiced, trained, measured, and enforced.

With the exception of Level 1, each maturity level is composed of key process areas that indicate where an organization should focus to improve its software process. The key process areas may be considered the requirements for achieving a maturity level. To achieve a maturity level, the key process areas for that level (and lower levels), must be satisfied and the process must be institutionalized. The key process areas at Level 2 focus on the software project's concerns related to establishing basic project management controls. Level 2 key process areas are:

- < Requirements Management
- < Software Project Planning
- < Software Project Tracking and Oversight
- < Software Subcontract Management
- < Software Quality Assurance
- < Software Configuration Management

Achieving the CMM for Software Level 2 maturity rating will allow HCFA to provide a more rapid response to mandated changes; reduce project management errors and miscalculations; accurately track project status and expectations; decrease software turnaround times and development costs and provide management visibility into software processes.

Some of the specific Key Process Areas associated with achieving the CMM for Software Level 2 maturity rating are discussed in the following Quality Assurance section of this IRM Plan.

**b. Quality Assurance**

HCFA has a need to develop a robust Quality Assurance (QA) process for all HCFA enterprise-wide systems. The purpose of QA is to provide management with appropriate visibility into the process being used by the software project and of products being built. QA involves reviewing and auditing the software products and activities to verify that they comply with the applicable procedures and standards and providing the software project and other appropriate managers with the results of these reviews and audits.

The five important activities that support Quality Assurance are: Change Management, Requirements Management (RM), Configuration Management (CM), Independent Verification and Validation (IV&V), and Independent Testing.

Change Management

HCFA has a need to develop a robust and effective Change Management process for its systems in order to better support its application development (and business) components with the task of implementing systems changes. Managing change in an IT environment is critical to efficiently maximizing investment dollars. Change Management is the vehicle by which HCFA will take control over the evolution of its hardware and software by establishing and enforcing a predictable life cycle for change implementation. Currently, there exists no common methodology for HCFA to systematically manage changes to hardware or software. The opportunity exists for HCFA to improve the systems development process by establishing a methodology and a group responsible for change management of systems hardware and software. An automated change management process will help HCFA track changes as they are requested, approved, planned, developed, tested, and implemented.

Requirements Management

HCFA has a need to develop a robust and effective Requirements Management process for its enterprise-wide systems. A related need exists to support the business and application development components with the task of developing systems requirements. The opportunity exists for HCFA to improve the systems development process by establishing a group of trained systems requirements

analysts and writers to fill a need that is not currently met by HCFA internal staff. Concurrent with requirements development, the management of systems requirements will help improve the quality of implemented systems by aiding the tracking of the requirements development and implementation process from

beginning to end: (i.e., from business requirements, to systems requirements, to test plans, to validation and to software implementation).

### Configuration Management

Configuration Management ensures that version control of system documentation and program code is institutionalized at HCFA in a central repository. A full configuration management environment will include: 1) version control during Development, Quality Assurance/Validation, Integration Testing and Production Implementation; 2) change tracking, so that developers and reviewers can identify changes made to the various software elements; and 3) sign-off by Development, Quality Assurance/Validation, Integration Testing and application owners during the various stages of the systems development life cycle. Although this activity was started in support of Y2K efforts, it is necessary to continue it into HCFA's future.

### Independent Verification and Validation

The purpose of this effort is to provide HCFA with IV&V services necessary for the efficient and effective management of its business information systems, infrastructure, and related information systems projects including, but not limited to legacy system enhancements and new systems development. The Agency's experience during the millennium project has also shown the value of having an independent evaluation of proposed plans and technical strategies from conceptualization through implementation.

### Independent Testing

The importance of effective testing has become evident in the Y2K initiatives. Pre-existing, non-Y2K related problems have been encountered during Y2K testing, more so than Y2K related problems themselves. It is impossible to calculate the cost of these error at this point in time, but this clearly demonstrates that HCFA needs a mechanism to ensure that systems have been fully exercised prior to implementation. It is equally important that HCFA be able to identify additional test requirements for those sections that have not been executed.

HCFA has lacked a means to measure testing quality prior to this initiative. For

this reason, HCFA plans to implement Independent Testing practices beyond the Y2K efforts. Test coverage and verification will be utilized to measure and analyze the quality of testing for all Medicare and Medicaid related systems. Independent Testing can also be a means for HCFA to perform a technical analysis of current and future systems.

#### **4. IT Training**

Existing staff are skilled and knowledgeable in the current IT environment. However, with the use of new database management systems, new program languages, and new access facilities, the Agency will need to both hire new staff with these skills and provide extensive training programs for existing staff. This responsibility falls under the CIO and OIS. There are a number of crosscutting business drivers that will impact the future hiring and retraining in these functional areas. OIS is committed to providing HCFA the ability to fully leverage the benefits which sound IT investments can provide in better-enabling the accomplishment of business objectives and improved customer (including beneficiary, partner, and stakeholder) services.

In FY2000, HCFA will invest in retraining staffs who have been focused exclusively on Y2K activities for the last several years. Programmers and system analysts who have been evaluating and renovating the Agency's legacy systems will need to be brought up to date on the direction of the future architecture and the technical skills needed to work in the new environment. The following is a list of the specific areas where training will be focused:

##### **a. Enterprise-wide IT Governance**

We need staff who are professionally trained in both the logical approach to and the highly proceduralized methods for supporting technical and financial analyses of projects. Specific skills are required in risk analysis, return on investment analysis, performance metrics (including earned-value), project planning and management--factor analysis, business requirements documentation, dependencies analysis; configuration/change management and requirements management; risk assessment and contingency planning.

##### **b. Infrastructure Operations**

HCFA must effectively plan and manage the HCFA IT infrastructure in the mainframe, mid-tier, network environments. We are moving more applications onto the mid-tier platform to use web-based technologies, to use the more desirable features of client-server computing and to gain more flexible arrangements for data storage and access. We must have the skills to effectively

implement and integrate mid-tier technologies into HCFA IT environment, and provide network integrity and computer security. To be effective as a mid-tier specialist requires knowledge of platforms (both servers and operating systems), inter-process and inter-platform communications (LANs, WANs, middleware) and the application environment (Web, 4th generation languages, objects, etc.). At the same time, a high-volume of our operations will reside on the mainframe and will continue to play a critical role. Critical skills needed are in communications operations to support both the networking (TCP/IP) and front-end protocols. Skills are needed to support internal processes, including mid-tier and specialized servers (e.g., storage, e-mail, security, network management), mainframe as servers, Unix servers, and shared resources across platforms.

Specific skills are required in network architecture and management technology, network and server security systems integration, systems engineering, cost-benefit analysis, tuning and performance, UNIX, C, C++, TCP/IP, JAVA, NT, per, and Web, and client-server/mid-tier.

#### **c. Database Development and Management**

To achieve the objectives of our IT vision we need skilled staff in modern database management approaches to develop or migrate databases that provide utility in supporting the business operations and policy/decision-making processes of the Agency. We need applications developers (1) who are skilled in using modern computer-assisted engineering (CASE) tools and developer toolkits to write for target environments such as the Web and assure platform independence via use of middleware; and (2) who understand the use of object technology and can aid us in determining its future within our operations and who are comfortable designing and fielding applications which are both inter-operable with components developed elsewhere in HCFA and inter-dependent on data store and structures for which they cannot dictate either logical structures or physical accesses. Further, HCFA needs to invest in higher-level data analysis skills to support its construction of the data warehouse/data marts/databases required to empower analysts and managers throughout HCFA. Staff needs training in JAVA and Web, client-server/mid-tier, UNIX, C, C++; message-oriented middleware; modern database technology and administration/management, including DB2, ORACLE, SQL (structured query language); and data mining, including decision support systems and on-line analysis processing.

#### **d. Data Quality, Integrity and Standards**

We must ensure that data used for operational and policy/decision-making is of

high quality (reliability and validity). Currently, we have minimal staff devoted to assuring the quality of HCFA's data, including protection of information at contractors and in transmission over networks. Since reliable and valid data is essential for both operational, research, and policy/decision-making, we must make a greater investment in staff resources devoted to the data quality area. Staff will be focused on EDI standards, HIPAA administrative simplification, and data quality and reliability.

**e. Security**

The movement to a more flexible and distributed, yet more integrated environment which includes Internet services substantially increases the risks to our systems operations and data. HCFA must ensure a sound and secure systems security environment, both for our internal and externally-maintained (contractor) systems. We must effectively plan the development of new IT solutions to business needs with security issues being considered as part of the development process and the development of network and operating systems. We need to acquire professional expertise in modern data security operations, including individuals with network and expertise in systems penetration and security auditing/testing, and awareness and security training/education. Our goal is to have a security posture wherein all resources are treated as virtual and risk assessment, auditing, automated intrusion detection, ethical hacking, and role-based access controls are standard tools. Specific systems security technical skills and training are needed in the following areas: technical vulnerability assessment; risk assessment, network security, Web/Internet security, intrusion detection, security auditing, security training.